Cyber Attack Protection and Control of Microgrids

Md Masud Rana, Li Li, and Steven W. Su

***Abstract*—Recently, the smart grid has been considered as a next-generation power system to modernize the traditional grid to improve its security, connectivity, efficiency and sustainability. Unfortunately, the smart grid is susceptible to malicious cyber attacks, which can create serious technical, economical, social and control problems in power network operations. In contrast to the traditional cyber attack minimization techniques, this paper proposes a recursive systematic convolutional (RSC) code and Kalman filter (KF) based method in the context of smart grids. Specifically, the proposed RSC code is used to add redundancy in the microgrid states, and the log maximum a-posterior is used to recover the state information, which is affected by random noises and cyber attacks. Once the estimated states are obtained by KF algorithm, a semidefinite programming based optimal feedback controller is proposed to regulate the system states, so that the power system can operate properly. Test results show that the proposed approach can accurately mitigate the cyber attacks and properly estimate and control the system states.**

***Index Terms*—Cyber attack, Kalman filter (KF), optimal feedback control, renewable microgrid, smart grid.**

I. Introduction

THE smart grid can provide an efficient way of supplying and consuming energy by providing two-way energy flow and communication [1]. It can integrate multiple renewable distributed energy resources (DERs) which are environment friendly, has low green house emission and is effective to alleviate transmission power losses. The associated connectivity and advanced information/communication infrastructure make the smart grid susceptible to cyber attacks [1], [2]. Statistics in the energy sector show that more than 150 cyber attacks happened in 2013 and 79 in 2014 [1]. As a result, the power outage cost is about $ 80 billion per year in the USA. Usually, the utility operators amortize it by increasing the energy tariff, which is unfortunately transferred to consumer expenses [3]. The renewable microgrid incorporating DERs can be a potential solution, but it needs to be properly monitored as its generation pattern depends on the weather and surrounding conditions. One of the smart grid features is that it can integrate multiple microgrids and monitor them using reliable communication networks.

Since the generation pattern of a microgrid varies on the time-place basis so its operating condition should be closely monitored. Therefore, the microgrid state estimation is an important function in the smart grid energy management system (EMS). As shown in Fig. 1 the system state estimation is an essential task for the monitoring and control of the power network. In order to monitor the grid information, the utility company has deployed a set of sensors around the smart grid. The communication infrastructure is used to send grid information from sensors to the EMS. The accurately estimated states can also be used in other functions of EMS such as contingency analysis, bad data detection, energy theft detection, stability analysis, and optimal power dispatch [4].

However, it is not economical or even infeasible to measure all states, so the state estimation is also a key task in this regard [5]. More importantly, cyber attacks can cause major social, economical and technical problems such as blackouts in power systems, tampering of smart meters reading and changing the forecasted load profiles [3]. These types of catastrophic phenomena are much easier to be committed in microgrids, so they create much more serious problems in the smart grid compared with the traditional grid [6]. Therefore, the system state estimation under cyber attacks for smart grids has drawn significant interests in the energy industry and signal processing based information and communication societies.

Many studies have been carried out to investigate the cyber attacks in smart grid state estimations. To begin with, most of the state estimation methods use the weighted least squared (WLS) technique under cyber attacks [7]−[9]. Chi-Square detector is also used to detect those attacks. Even though this approach is easy to be implemented for nonlinear systems, it is computationally intensive and it cannot eliminate the attacks properly [5], [7]. To this end, the WLS based l_1 optimization method is explored in [4]. Furthermore, a new detection scheme to detect the false data injection attack is proposed in [2]. It employs a Kullback-Leibler method to calculate the distance between the probability distributions derived from the observation variations. A sequential detection of false data injection in smart grids is investigated in [2]. It adopts a centralized detector based on the generalized likelihood ratio and cumulative sum algorithm. Note that this detector usually depends on the parametric inferences so is inapplicable to the nonparametric inferences [10]. A semidefinite programming based AC power system state estimation is proposed in [11]. Thereafter, a Kalman filter (KF) based microgrid energy theft detection algorithm is presented in [3].

A lot of efforts have been devoted towards the power system state estimation under the condition of unreliable communication channels. Generally, the attackers have limited attacking energy to jam the channel in order to achieve the desired goals [12]. So, the sensor data scheduling for state estimation with energy constraints is studied in [13]. In this research, the sensor has to decide whether to send its data to

Manuscript received November 2, 2015; accepted May 25, 2016. Recommended by Associate Editor Qinmin Yang. *(Corresponding author: Md Masud Rana.)*

Citation: M. M. Rana, L. Li, and S. W. Su, "Cyber attack protection and control of microgrids," *IEEE/CAA J. of Autom. Sinica*, vol. 5, no. 2, pp. 602−609, Mar. 2018.

The authors are all with the Faculty of Engineering and Information Technology, University of Technology Sydney, Broadway, NSW 2007, Australia (e-mail: 11766084@student.uts.edu.au; li.li@uts.edu.au; steven.su@uts.edu.au).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JAS.2017.7510655

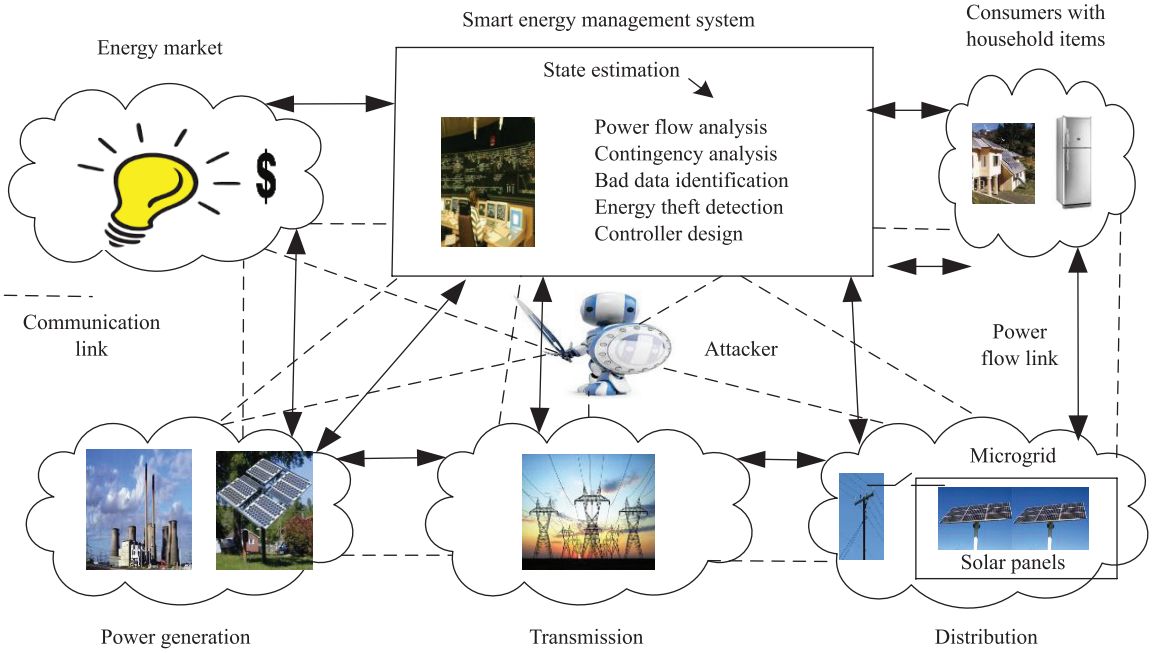

Fig. 1. Flow of electricity and information between different sections of smart grid [3].

a remote estimator or not based on its energy and estimation error covariance matrix. This idea is further extended in [14], where both the sensor and attacker have energy constraints for sending information. The considered attack is on the communication channel between a sensor and a remote estimator. Basically, the sensor aims to minimize the average estimation error covariance matrix, while attackers try to maximize it. So, an iterative game theory is used to solve the optimization problem. Due to the motivation of unknown attacking patterns, authors in [12], [15] investigated how the attacker can design the attacking policy so the estimation performance can be deteriorated. Then the average estimation error covariance based optimal scheduling strategy is proposed to avoid such kind of attacks.

Many feedback control algorithms have been proposed to regulate the system. The linear quadratic Gaussian (LQG) based detecting techniques for cyber integrity attacks on the sensors of a control system is proposed in [12], [16]. It shows that the residual error based chi-squared detection technique is not suitable when the attacker does not know the system dynamics. Based on this analysis, they consider the cyber attack model as an i.i.d (independent, identically distributed) Gaussian distribution, and then the LQG objective function is modified. At the end, they developed a sufficient condition to detect the false alarm probability and proposed an optimization algorithm to minimize it. In [17], a new strategy is recommended for designing a communication and control infrastructure in a distribution system based on the virtual microgrid concept. It is shown in [18], [19] that designing a state feedback control framework for a general case of polynomial discrete-time system is quite challenging because the solution is non-convex. Thus, the convex optimization based controller design has gained growing interest in the research community.

The key contributions of this paper are summarized as follows:

1) A microgrid incorporating multiple distributed energy resources (DERs) is modeled as a discrete time linear state-space equation considering the uncertainty and cyber attack in the measurement.

2) A recursive systematic convolutional (RSC) code is proposed to mitigate the impairments and introduce redundancy in the system states. The log maximum a posterior is adopted to recover the state information which is affected by random noises and cyber attacks.

3) After estimating the system states, a feedback control strategy for voltage regulation of the microgrid is proposed based on semidefinite programming. This proposed control scheme acts as a precursor in terms of network stability and the operation of DERs.

The remainder of this paper is organized as follows. A microgrid system model is presented in Section II. The observation model and cyber attack process are described in Section III. Moreover, the KF based dynamic state estimation is described in Section IV. The proposed control technique is derived in Section V, followed by the simulation results and discussions in Section VI. Finally, the paper is wrapped up with conclusions and future work in Section VII.

Notations: Bold face lower and upper case letters are used to represent vectors and matrices, respectively; $\boldsymbol{x}'$ denotes the transpose of $\boldsymbol{x}$, $E(\cdot)$ denotes the expectation operator and $\boldsymbol{I}$ is the identity matrix.

II. Microgrid System Model

The considered N micro-sources in this study are connected to the main grid. For simplicity, we assume that $N = 4$ solar panels are connected through the IEEE-4 bus test feeder as shown in Fig. 2 [20], [21]. Here, the input voltages are denoted by $\boldsymbol{v}_p = (v_{p1}\ v_{p2}\ v_{p3}\ v_{p4})'$, where v_{pi} is the ith DER input voltage. The four micro-sources are connected to the power

network at the corresponding points of common coupling (PCCs) whose voltages are denoted by $\boldsymbol{v}_s = (v_1\ v_2\ v_3\ v_4)'$, where v_i is the ith point of common coupling (PCC) voltage.

Now by applying Laplace transformation, the nodal voltage equation can be obtained:

$$\boldsymbol{Y}(s)\boldsymbol{v}_s(s) = \frac{1}{s}\boldsymbol{L}_c^{-1}\boldsymbol{v}_p(s) \tag{1}$$

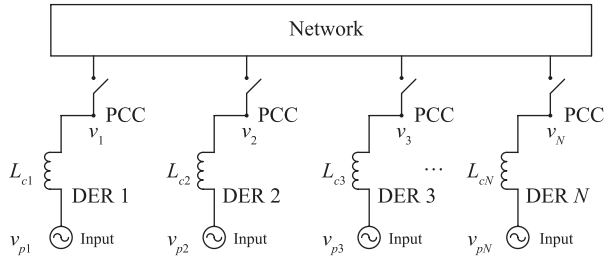

Fig. 2. Micro-sources are connected to the power network [21].

where $\boldsymbol{L}_c = \text{diag}\{L_{c_1},\ L_{c_2},\ L_{c_3},\ L_{c_4}\}$ and $\boldsymbol{Y}(s)$ is the admittance matrix of the entire power network incorporating four micro-sources [21]. Now we can convert the transfer function form into the linear state-space model [21]. The discrete-time linear dynamic system can be derived as follows:

$$\boldsymbol{x}(k+1) = \boldsymbol{A}_d\boldsymbol{x}(k) + \boldsymbol{B}_d\boldsymbol{u}(k) + \boldsymbol{n}_d(k) \tag{2}$$

where $\boldsymbol{x}(k) = \boldsymbol{v}_s - \boldsymbol{v}_{\text{ref}}$ is the PCC state voltage deviation, $\boldsymbol{v}_{\text{ref}}$ is the PCC reference voltage, $\boldsymbol{u}(k) = \boldsymbol{v}_p - \boldsymbol{v}_{\text{pref}}$ is the DER control input deviation, $\boldsymbol{v}_{\text{pref}}$ is the reference control effort, $\boldsymbol{n}_d(k)$ is the zero mean process noise whose covariance matrix is $\boldsymbol{Q}_n$, the state matrix $\boldsymbol{A}_d = \boldsymbol{I} + \boldsymbol{A}\Delta t$ and input matrix $\boldsymbol{B}_d = \boldsymbol{B}\Delta t$ with

$$\boldsymbol{A} = \begin{bmatrix} 175.9 & 176.8 & 511 & 103.6 \\ -350 & 0 & 0 & 0 \\ -544.2 & -474.8 & -408.8 & -828.8 \\ -119.7 & -554.6 & -968.8 & -1077.5 \end{bmatrix} \tag{3}$$

$$\boldsymbol{B} = \begin{bmatrix} 0.8 & 334.2 & 525.1 & -103.6 \\ -350 & 0 & 0 & 0 \\ -69.3 & -66.1 & -420.1 & -828.8 \\ -434.9 & -414.2 & -108.7 & -1077.5 \end{bmatrix} \tag{4}$$

and Δt is the discretization parameter. For discretizing a continuous-time system into a discrete-time system, there are several techniques available in the literature such as traditional approximation method, delta operator and shift operator [22]−[25]. Similar to [22], [25], this paper adopts the traditional approximation method ignoring discretization errors. In the following section, the observation model and attack process is explored.

III. Observation Model and Cyber Attack

The measurements of the microgrid states are obtained by a set of sensors and can be modeled as follows:

$$\boldsymbol{z}(k) = \boldsymbol{C}\boldsymbol{x}(k) + \boldsymbol{w}(k) \tag{5}$$

where $\boldsymbol{z}(k)$ is the measurements, $\boldsymbol{C}$ is the measurement matrix and $\boldsymbol{w}(k)$ is the zero mean sensor measurement noise whose covariance matrix is $\boldsymbol{R}_w$. Generally, the objective of attackers is to insert false data into the observations as follows:

$$\boldsymbol{y}(k) = \boldsymbol{C}\boldsymbol{x}(k) + \boldsymbol{w}(k) + \boldsymbol{a}(k) \tag{6}$$

where $\boldsymbol{a}(k)$ is the false data inserted by the attacker [1]−[3]. The attackers have complete access to the system infrastructure so that they can hijack, record and manipulate data according to their best interest. In this paper, the cyber attack pattern is similar to those illustrated in [1], [2], [26]. Fig. 3 shows the observation model and cyber attack process in the context of smart grid state estimations.

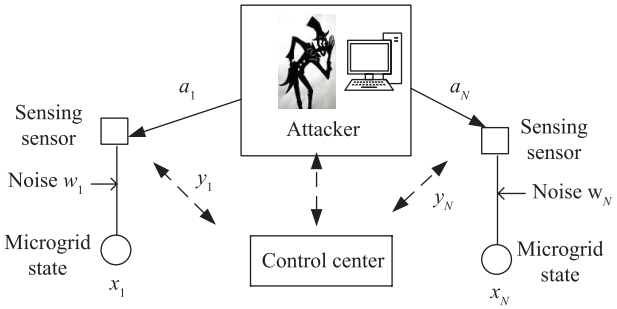

Fig. 3. Observation model with cyber attack in the microgrid.

To secure the system states, in the signal processing research community, the channel code is used. Motivated by the convolutional coding concept [27], [28], the microgrid state-space and observation models are regarded as the outer code. Then, the standard uniform quantizer performs quantization to get the sequence of bits $\boldsymbol{b}(k)$. $\boldsymbol{b}(k)$ is encoded by RSC channel code which is regarded as the inner code. The main reason for using RSC code is to mitigate impairments and introduce redundancy in the system to protect the grid information. Generally speaking, RSC code is characterized by three parameters: the codeword length n, the message length l, and the constraint length m, i.e., (n, l, m). The quantity l/n refers to the code rate which indicates the amount of parity bits added to the data stream. The constraint length specifies $m-1$ memory elements which represents the number of bits in the encoder memory that affects the RSC generation output bits. If the constraint length m increases, the encoding process intrinsically needs a longer time to execute the logical operations. Other advantages of the RSC code compared with the convolutional and turbo encoder include its reduced computation complexity, systematic output features and no error floor [29]. From this point of view, this paper considers a (2, 1, 3) RSC code and (1 0 1, 1 1 1) code generator polynomial in the feedback process. According to the RSC features, the code rate is $1/2$ and there are two memories in the RSC process. As shown in Fig. 4, this RSC code produces two outputs and can convert an entire data stream into one single codeword [30]. The codeword is then passed through the binary phase shift keying (BPSK) to obtain $\boldsymbol{s}(k)$. $\boldsymbol{s}(k)$ is passed through the additive white Gaussian noisy (AWGN) channel. To illustrate, Fig. 4 shows the proposed cyber attack protection procedure in the context of smart grids.

At the end, the received signal is:

$$\boldsymbol{r}(k) = \boldsymbol{s}(k) + \boldsymbol{e}(k) \tag{7}$$

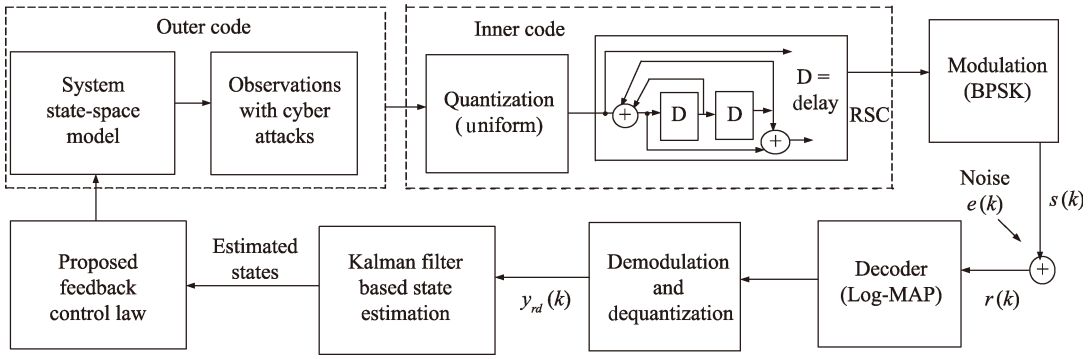

Fig. 4. An illustration of the cyber attack protection in smart grids.

where $\boldsymbol{e}(k)$ is the AWGN noise. The received signal is followed by the log-maximum a posteriori (Log-MAP) decoding for this dynamic system. The Log-MAP works recursively from the forward path to the backward path to recover the state information [27]. The Log-MAP output information is sent for demodulation and dequantization processes, followed by the state estimation scheme.

IV. Proposed Framework for Cyber Attack Minimization in Smart Grids

The proposed framework uses the KF to estimate the system states in the context of smart grids. The KF operates recursively on observation information to produce the optimal state estimation. Generally, the forecasted system state estimate is expressed as follows [31]:

$$\hat{\boldsymbol{x}}^{-}(k) = \boldsymbol{A}_d\hat{\boldsymbol{x}}(k-1) + \boldsymbol{B}_d\boldsymbol{u}(k-1) \tag{8}$$

where $\hat{\boldsymbol{x}}(k-1)$ is the estimated state of the last step. Then the forecasted error covariance matrix is given by:

$$\boldsymbol{P}^{-}(k) = \boldsymbol{A}_d\boldsymbol{P}(k-1)\boldsymbol{A}_d' + \boldsymbol{Q}_n(k-1) \tag{9}$$

where $\boldsymbol{P}(k-1)$ is the estimated error covariance matrix of the last step. The observation innovation residual $\boldsymbol{d}(k)$ is given by:

$$\boldsymbol{d}(k) = \boldsymbol{y}_{rd}(k) - \boldsymbol{C}\hat{\boldsymbol{x}}^{-}(k) \tag{10}$$

where $\boldsymbol{y}_{rd}(k)$ is the dequantized and demodulated output bit sequence. The Kalman gain matrix can be written as:

$$\boldsymbol{K}(k) = \boldsymbol{P}^{-}(k)\boldsymbol{C}'[\boldsymbol{C}\boldsymbol{P}^{-}(k)\boldsymbol{C}' + \boldsymbol{R}_w(k)]^{-1}. \tag{11}$$

The updated state estimation is given by:

$$\hat{\boldsymbol{x}}(k) = \hat{\boldsymbol{x}}^{-}(k) + \boldsymbol{K}(k)\boldsymbol{d}(k). \tag{12}$$

Finally, the updated estimated error covariance matrix $\boldsymbol{P}(k)$ is expressed as follows:

$$\boldsymbol{P}(k) = \boldsymbol{P}^{-}(k) - \boldsymbol{K}(k)\boldsymbol{C}\boldsymbol{P}^{-}(k). \tag{13}$$

After estimating the system state, the proposed control strategy is applied for regulating the microgrid states as shown in the next section.

V. Proposed Optimal Feedback Controller

In the simulation section, it has been shown that the proposed method is able to well estimate the system states. So, here we assume the microgrid state information is available. In order to regulate the microgrid states, define the following feedback control law [32]−[34]:

$$\boldsymbol{u}(k) = \boldsymbol{F}\boldsymbol{x}(k) \tag{14}$$

by minimizing the following cost function:

$$J = E\Big[\lim_{N\to\infty}\frac{1}{N}\sum_{k=0}^{N-1}\{\boldsymbol{x}'(k)\boldsymbol{Q}_z\boldsymbol{x}(k) + \boldsymbol{u}'(k)\boldsymbol{R}_z\boldsymbol{u}(k)\}\Big] \tag{15}$$

where $E(\cdot)$ denotes the expectation operator and $\boldsymbol{F}$ is the state feedback gain matrix, $\boldsymbol{Q}_z$ and $\boldsymbol{R}_z$ are positive-definite state weighting matrix and control weighting matrix.

Then the closed loop system is:

$$\boldsymbol{x}(k+1) = (\boldsymbol{A}_d + \boldsymbol{B}_d\boldsymbol{F})\boldsymbol{x}(k) + \boldsymbol{n}_d(k). \tag{16}$$

By using (14) and standard trace operator ($m'Dn = \mathrm{tr}[Dnm']$), (15) can be expressed as:

$$\begin{aligned} J =& E\Big[\lim_{N\to\infty}\frac{1}{N}\sum_{k=0}^{N-1}\mathrm{tr}\{\boldsymbol{Q}_z\boldsymbol{x}(k)\boldsymbol{x}'(k) + \boldsymbol{F}'\boldsymbol{R}_z\boldsymbol{F}\boldsymbol{x}(k)\boldsymbol{x}'(k)\}\Big] \\ =& \mathrm{tr}\Big[\boldsymbol{Q}_z + \boldsymbol{F}'\boldsymbol{R}_z\boldsymbol{F}\Big]\boldsymbol{P} \end{aligned} \tag{17}$$

where $\boldsymbol{P} = E\Big[\lim_{N\to\infty}\frac{1}{N}\sum_{k=0}^{N-1}\boldsymbol{x}(k)\boldsymbol{x}'(k)\Big]$ and it can be written as follows:

$$\begin{aligned} \boldsymbol{P} =& E\Big[\lim_{N\to\infty}\frac{1}{N}\sum_{k=0}^{N-2}\boldsymbol{x}(k+1)\boldsymbol{x}'(k+1)\Big] + \lim_{N\to\infty}\frac{1}{N}E[\boldsymbol{x}(0)\boldsymbol{x}'(0)] \\ =& E\Big[\lim_{N\to\infty}\frac{1}{N}\sum_{k=0}^{N-2}(\boldsymbol{A}_d+\boldsymbol{B}_d\boldsymbol{F})\boldsymbol{x}(k)\boldsymbol{x}'(k)(\boldsymbol{A}_d+\boldsymbol{B}_d\boldsymbol{F})'\Big] + \boldsymbol{Q}_n. \end{aligned} \tag{18}$$

Then (18) can be written as follows:

$$\boldsymbol{P} = (\boldsymbol{A}_d + \boldsymbol{B}_d\boldsymbol{F})\boldsymbol{P}(\boldsymbol{A}_d + \boldsymbol{B}_d\boldsymbol{F})' + \boldsymbol{Q}_n. \tag{19}$$

Now one can consider the following inequality,

$$\begin{aligned} &(\boldsymbol{A}_d + \boldsymbol{B}_d\boldsymbol{F})\boldsymbol{P}(\boldsymbol{A}_d + \boldsymbol{B}_d\boldsymbol{F})' - \boldsymbol{P} + \boldsymbol{Q}_n < \boldsymbol{0} \\ &(\boldsymbol{A}_d + \boldsymbol{B}_d\boldsymbol{F})\boldsymbol{P}\boldsymbol{P}^{-1}\boldsymbol{P}(\boldsymbol{A}_d + \boldsymbol{B}_d\boldsymbol{F})' - \boldsymbol{P} + \boldsymbol{Q}_n < \boldsymbol{0}. \end{aligned} \tag{20}$$

Now one can introduce a new variable $\boldsymbol{H} = \boldsymbol{FP}$ and rewrite the (20) as follows:

$$(\boldsymbol{A}_d\boldsymbol{P} + \boldsymbol{B}_d\boldsymbol{H})\boldsymbol{P}^{-1}(\boldsymbol{A}_d\boldsymbol{P} + \boldsymbol{B}_d\boldsymbol{H})' - \boldsymbol{P} + \boldsymbol{Q}_n < \boldsymbol{0}. \quad (21)$$

Now according to the Schur's complement, (21) can be transformed into the following form:

$$\begin{bmatrix} \boldsymbol{Q}_n - \boldsymbol{P} & \boldsymbol{A}_d\boldsymbol{P} + \boldsymbol{B}_d\boldsymbol{H} \\ (\boldsymbol{A}_d\boldsymbol{P} + \boldsymbol{B}_d\boldsymbol{H})' & -\boldsymbol{P} \end{bmatrix} < \boldsymbol{0}. \quad (22)$$

From (17), F and P can be found by minimising the following expression:

$$\begin{aligned} &\underset{\boldsymbol{P},\boldsymbol{F}}{\text{minimise}} \quad \text{tr}[\boldsymbol{Q}_z + \boldsymbol{F}'\boldsymbol{R}_z\boldsymbol{F}]\boldsymbol{P} \\ &\text{s. t.} \qquad (22). \end{aligned} \quad (23)$$

Based on the $\boldsymbol{H} = \boldsymbol{FP}$, (23) can be transformed as follows:

$$\underset{\boldsymbol{P},\boldsymbol{S},\boldsymbol{H}}{\text{minimise}} \quad \text{tr}[\boldsymbol{Q}_z\boldsymbol{P}] + \text{tr}[\boldsymbol{S}] \quad (24)$$

$$\text{s. t.} \quad \boldsymbol{S} > \boldsymbol{R}_z^{\frac{1}{2}}\boldsymbol{H}\boldsymbol{P}^{-1}\boldsymbol{H}'\boldsymbol{R}_z^{\frac{1}{2}} \quad (25)$$

$$\text{Hold } (22).$$

According to the Schur's complement, we can rewrite (25) as follows:

$$\begin{bmatrix} \boldsymbol{S} & \boldsymbol{R}_z^{\frac{1}{2}}\boldsymbol{H} \\ \boldsymbol{H}'\boldsymbol{R}_z^{\frac{1}{2}} & \boldsymbol{P} \end{bmatrix} > \boldsymbol{0}. \quad (26)$$

Then we can formulate the proposed optimization problem as follows [30]:

$$\begin{aligned} &\underset{\boldsymbol{P},\boldsymbol{S},\boldsymbol{H}}{\text{minimise}} \quad \text{tr}[\boldsymbol{Q}_z\boldsymbol{P}] + \text{tr}[\boldsymbol{S}] \\ &\text{s. t.} \qquad \text{Hold } (22), \text{Hold } (26). \end{aligned} \quad (27)$$

Finally, the feedback gain matrix is computed as:

$$\boldsymbol{F} = \boldsymbol{H}\boldsymbol{P}^{-1}. \quad (28)$$

The proposed convex problem can be solved effectively and efficiently using a number of available softwares such as YALMIP [35].

VI. Performance Evaluation

In this section, we evaluate the performance of the proposed approaches under cyber attacks in smart grids. An overall system level diagram for system state estimation and control is illustrated in Fig. 5. After sensing and quantizing the system states, RSC code is proposed to add redundancy into the data stream in a controlled manner to give the Log-MAP decoder to correct errors at EMS. Once the estimated system states are obtained, a semidefinite programming based optimal feedback controller is proposed to regulate the system states [30]. The simulation is performed using the microgrid connected to IEEE 4-bus distribution feeder. The simulation parameters are summarized in Table I.

The mean squared error (MSE) versus signal-to-noise ratio (SNR) is presented in Fig. 6. It can be observed that the proposed method provides significant performance improvement compared with the existing method [1]. The reason is that the RSC code is used to protect the system from cyber attacks and noises by adding redundancy in the system states. It can also protect the state information from the unreliable lossy communication networks. Furthermore, the Log-MAP decoding can also facilitate the accurate extraction of the system state. For better visualization of the cyber attack, the states versus time step are illustrated in Figs. 7−10. It can be observed and expected that the cyber attack still affects the system states seriously when the existing method is used to estimate system states [1]. In other words, there is a significant fluctuation due to the random noises and cyber attacks. Interestingly, the proposed RSC based cyber attack protection technique can tolerate the system impairments by introducing redundancy and protection in the system states. As a result, the proposed method can estimate microgrid states accurately even if there are cyber attacks and noises.

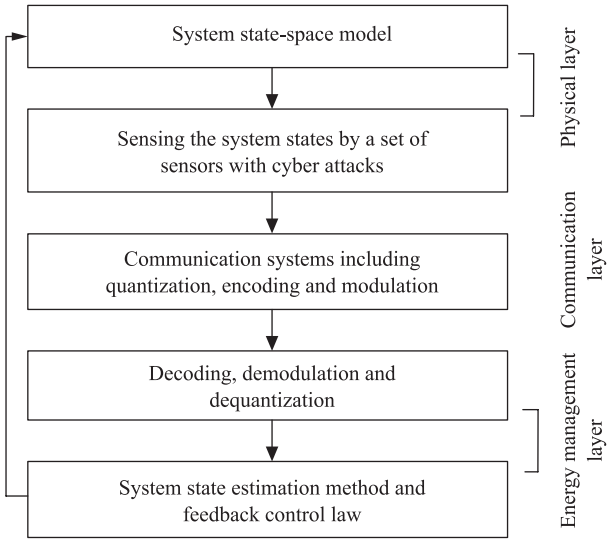

Fig. 5. System level diagram for system state estimation and control.

TABLE I
Parameters for the Simulation

Parameters	Values	Parameters	Values
$\boldsymbol{Q}_z$	$\text{diag}\{10^{-2}, 10^{-2}, 10^{1}, 10^{-3}\}$	$\boldsymbol{R}_z$	$0.01 * \boldsymbol{I}_4$
Codes generator	$5/7$	Δt	0.0001
Quantization	Uniform 16 bits	Decoding	Log-MAP
Code rate	$1/2$	Channel	AWGN
$\boldsymbol{Q}_n$	$0.005 * \boldsymbol{I}_4$	$\boldsymbol{R}_w$	$0.05 * \boldsymbol{I}_4$

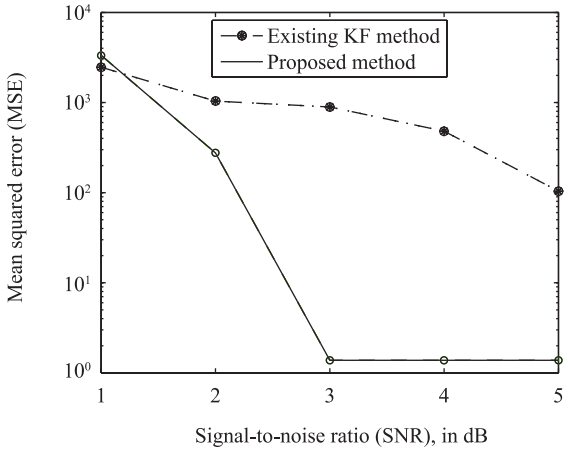

Fig. 6. MSE versus SNR performance comparison using microgrid.

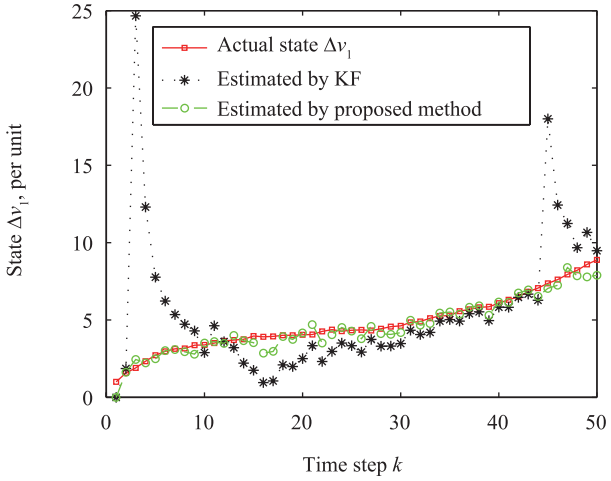

Fig. 7. State trajectory of Δv_1 and its estimate.

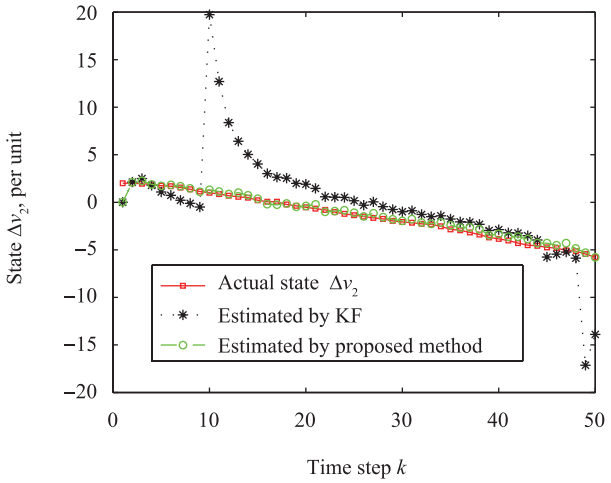

Fig. 8. State trajectory of Δv_2 and its estimate.

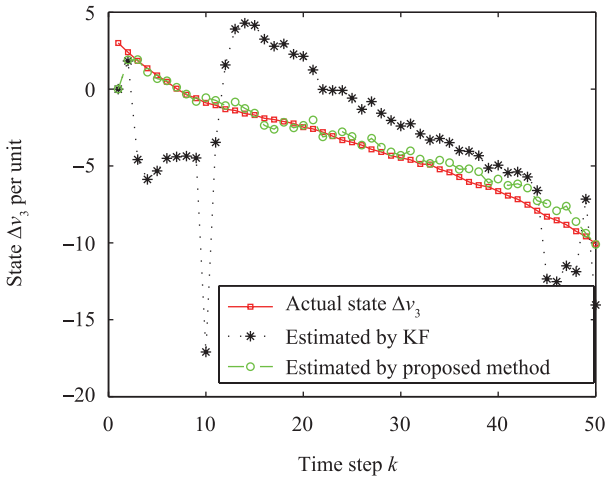

Fig. 9. State trajectory of Δv_3 and its estimate.

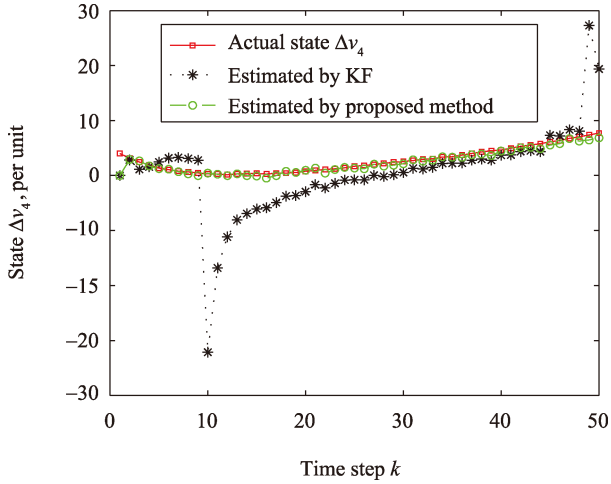

Fig. 10. State trajectory of Δv_4 and its estimate.

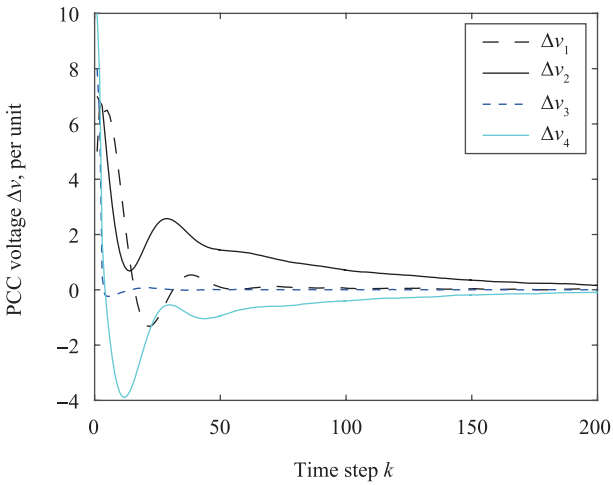

Fig. 11. Controlling the states trajectory.

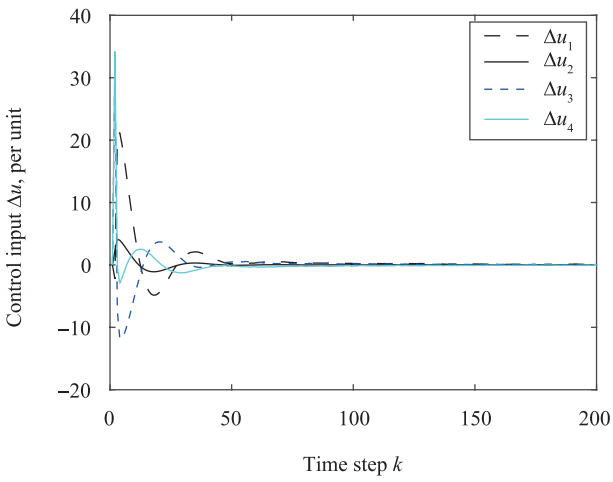

Fig. 12. Control input trajectory.

Unfortunately, it is noticed that the actual PCC state deviations increase dramatically (Figs. 7−10), which is very dangerous in terms of network stability and microgrid operation. Thus, it is necessary to apply a suitable control technique, so that the PCC voltage deviations are driven to zero. After applying the proposed control method to the microgrid connected to the IEEE 4-bus distribution system, it can be seen from Figs. 11 and 12 that the proposed controller is able to keep

the voltage deviations to zero by the time k = 200, which acts as a precursor in terms of network stability and proper operation of microgrids. Besides, the corresponding control input of each DER is shown in Fig. 12, which implies that it requires a small amount of control input.

VII. Conclusion

This paper proposes a cyber attack minimization based dynamic state estimation technique and feedback control algorithm in smart grids. An RSC coded cyber attack protection technique is proposed to add redundancy in the system states. Then a Log-MAP decoding can assist to extract the system states from the received signal which is polluted by random noises and cyber attacks. In order to regulate the voltage deviation, this study proposes a semidefinite programming based optimal feedback control method. The effectiveness of the developed approaches is verified by numerical simulations. These findings can help to design the future smart control center under cyber attacks. Consequently, it is encouraged to use an environmentally friendly renewable microgrid and the utility operator can monitor and control the power network properly. In the future work, packet losses and delay will be investigated in terms of system performance.

References

[1] D. B. Rawat and C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Process. Lett.*, vol. 22, no. 10, pp. 1652−1656, Oct. 2015.

[2] S. Li, Y. Y. lmaz, and X. D. Wang, "Quickest detection of false data injection attack in wide-area smart grids," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2725−2735, Nov. 2015.

[3] M. Esmalifalak, G. Shi, Z. Han, and L. Y. Song, "Bad data injection attack and defense in electricity market using game theory study," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 160−169, Mar. 2013.

[4] K. C. Sou, H. Sandberg, and K. H. Johansson, "On the exact solution to a smart grid cyber-security analysis problem," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 856−865, Jun. 2013.

[5] M. Esmalifalak, H. Nguyen, R. Zheng, and Z. Han, "Stealth false data injection using independent component analysis in smart grid," in *Proc. Int. Conf. Smart Grid Communications*, Brussels, Belgium, 2011, pp. 244−248.

[6] S. A. Salinas, and P. Li, "Privacy-preserving energy theft detection in microgrids: A state estimation approach," *IEEE Trans. Power Syst.*, vol. 31, no. 2, pp. 883−894, Mar. 2016.

[7] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362−1370, Sep. 2012.

[8] A. Alimardani, F. Therrien, D. Atanackovic, J. Jatskevich, and E. Vaahedi, "Distribution system state estimation based on nonsynchronized smart meters," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2919−2928, Nov. 2015.

[9] S. Meliopoulos, R. K. Huang, E. Polymeneas, and G. Cokkinides, "Distributed dynamic state estimation: Fundamental building block for the smart grid," in *Proc. Power & Energy Society General Meeting*, Denver, CO, USA, 2015, pp. 1−6.

[10] C. J. Gu, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in AC state estimation," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2476−2483, Sep. 2015.

[11] Y. Weng, Q. Li, R. Negi, and M. Ilić, "Distributed algorithm for SDP state estimation," in *Proc. IEEE PES Innovative Smart Grid Technologies*, Washington, DC, USA, 2013, pp. 1−6.

[12] H. Zhang, P. Cheng, L. Shi, and J. M. Chen, "Optimal denial-of-service attack scheduling with energy constraint," *IEEE Trans. Automat. Control*, vol. 60, no. 11, pp. 3023−3028, Nov. 2015.

[13] L. Shi, P. Cheng, and J. M. Chen, "Sensor data scheduling for optimal state estimation with communication energy constraint," *Automatica*, vol. 47, no. 8, pp. 1693−1698, Aug. 2011.

[14] Y. Z. Li, L. Shi, P. Cheng, J. M. Chen, and D. E. Quevedo, "Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach," *IEEE Trans. Automat. Control*, vol. 60, no. 10, pp. 2831−2836, Oct. 2015.

[15] H. Zhang, P. Cheng, L. Shi, and J. M. Chen, "Optimal dos attack policy against remote state estimation," in *Proc. 52nd Annu. Conf. Decision and Control*, Firenze, Italy, 2013, pp. 5444−5449.

[16] Y. L. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on SCADA systems," *IEEE Trans. Control Syst. Technol.*, vol. 22, no. 4, pp. 1396−1407, Jul. 2014.

[17] S. A. Arefifar, A. R. I. Mohamed, T. El-Fouly, "Optimized multiple microgrid-based clustering of active distribution systems considering communication and control requirements," *IEEE Trans. Ind. Electron.*, vol. 62, no. 2, pp. 711−723, Feb. 2015.

[18] S. Saat, S. K. Nguang, J. Wu, and G. B. Zeng, "Disturbance attenuation for a class of uncertain polynomial discrete-time systems: An integrator approach," in *Proc. 12th Int. Conf. Control Automation Robotics & Vision*, Guangzhou, China, 2012, pp. 787−792.

[19] N. Azman, S. Saat, and S. K. Nguang, "Nonlinear observer design with integrator for a class of polynomial discrete-time systems," in *Proc. Int. Conf. Computer, Communications, and Control Technology*, Kuching, Malaysia, 2015, pp. 422−426.

[20] H. J. Li, F. X. Li, Y. Xu, D. T. Rizy, and J. D. Kueck, "Adaptive voltage control with distributed energy resources: Algorithm, theoretical analysis, simulation, and field test verification," *IEEE Trans. Power Syst.*, vol. 25, no. 3, pp. 1638−1647, Aug. 2010.

[21] H. S. Li, L. F. Lai, and H. V. Poor, "Multicast routing for decentralized control of cyber physical systems with an application in smart grid," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 6, pp. 1097−1107, Jul. 2012.

[22] E. Ghahremani and I. Kamwa, "Online state estimation of a synchronous generator using unscented Kalman filter from phasor measurements units," *IEEE Trans. Energy Conv.*, vol. 26, no. 4, pp. 1099−1108, Dec. 2011.

[23] D. Buchstaller, E. C. Kerrigan, and G. A. Constantinides, "Sampling and controlling faster than the computational delay," *IET Control Theory Appl.*, vol. 6, no. 8, pp. 1071−1079, May 2012.

[24] H. J. Yang, Y. Q. Xia, P. Shi, and M. Y. Fu, "A novel delta operator Kalman filter design and convergence analysis," *IEEE Trans. Circ. Syst. I: Reg. Pap.*, vol. 58, no. 10, pp. 2458−2468, Oct. 2011.

[25] T. J. Sui, K. Y. You, M. Y. Fu, and D. Marelli, "Stability of MMSE state estimators over lossy networks using linear coding," *Automatica*, vol. 51, pp. 167−174, Jan. 2015.

[26] S. Ntalampiras, "Detection of integrity attacks in cyber-physical critical

infrastructures using ensemble modeling," *IEEE Trans. Ind. Inf.*, vol. 11, no. 1, pp. 104−111, Feb. 2015.

[27] Y. Jing, *A Practical Guide to Error-Control Coding Using MATLAB*. Boston, London, UK: Artech House, 2010.

[28] S. P. Gong, H. S. Li, L. F. Lai, and R. C. Qiu, "Decoding the 'nature encoded' messages for distributed energy generation control in microgrid," in *Proc. IEEE Int. Conf. Communications*, Kyoto, Japan, 2011, pp. 1−5.

[29] C. Vlădeanu and S. El Assad, *Nonlinear Digital Encoders for Data Communications*. New York, USA: John Wiley & Sons, 2014.

[30] M. M. Rana, L. Li, and S. W. Su, "Cyber attack protection and control in microgrids using channel code and semidefinite programming," in *Proc. Power and Energy Society General Meeting*, Boston, MA, USA, 2016, pp. 1−5.

[31] D. Simon, *Optimal State Estimation: Kalman, H Infinity, and Nonlinear Approaches*. New Jersey, USA: John Wiley & Sons, 2006.

[32] A. K. Singh, R. Singh, and B. C. Pal, "Stability analysis of networked control in smart grids," *IEEE Trans. Smart Grid*, vol. 6, no. 1, pp. 381−390, Jan. 2015.

[33] C. Olalla, R. Leyva, A. El Aroudi, and I. Queinnec, "Robust LQR control for PWM converters: An LMI approach," *IEEE Trans. Ind. Electron.*, vol. 56, no. 7, pp. 2548−2558, Jul. 2009.

[34] M. Fardad and M. R. Jovanović, "On the design of optimal structured and sparse feedback gains via sequential convex programming," in *Proc. American Control Conf.*, 2014, Portland, OR, USA, pp. 2426−2431.

[35] J. Löfberg, "YALMIP: A toolbox for modeling and optimization in MATLAB," in *Proc. IEEE Int. Symp. Computer Aided Control Systems Design*, Taipei, China, 2004, pp. 284−289.

Md Masud Rana is at the School of Electrical, Mechanical and Mechatronic Systems, University of Technology Sydney, Australia. His research interests include theoretical and algorithmic studies in signal processing and optimizations, statistical learning and inferences for high dimensional data, distributed optimizations and adaptive algorithms, as well as their applications in communications, networked systems and smart grid.

Li Li received the Ph.D. degree from the University of California, USA. He is serving as a Senior Lecturer at the School of Electrical, Mechanical and Mechatronic Systems, University of Technology Sydney, Australia. His current research interests include robust control systems, distributed model predictive control of power systems, model reduction of power systems, control on microgrids, vehicle-to-grid coordination method and smart grid market.

Steven W. Su received the Ph.D. degree in control engineering from the Australian National University in May 2003. He was then a Research Fellow for nearly four years at the Faculty of Engineering at the University of NSW. His research interests include biomedical instrumentation, physiological variable modeling, data acquisition and distribution, process control and system identification. He is currently an Associate Professor at the School of EMMS, and a core member of the Center for Health Technologies at UTS.